AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

Claim 1 (currently amended): A system for decrypting an encrypted computer program including at least one first block and a plurality of second blocks in sequence, the system comprising:

means for generating a first cipher key from the at least one first block of the encrypted computer program;

means for performing a first decryption ~~of a plurality~~on each of the plurality of second blocks of the encrypted computer program with said first cipher key which is generated from the at least one first block;

means for performing a second decryption ~~of~~ on each of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key.

Claim 2 (previously presented): The system as set forth in claim 1, wherein said at least one first block is not encrypted.

Claim 3 (previously presented): The system as set forth in claim 1,

wherein said plurality of second blocks are encrypted at least with said first cipher key prior to being decrypted.

Claim 4 (previously presented): The system as set forth in claim 3,

wherein at least one of said plurality of second blocks is encrypted with said second cipher key prior to being decrypted.

Claim 5 (previously presented): The system as set forth in claim 1, further comprising:

means for determining whether the encrypted computer program is analyzed; and

means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed.

Claim 6 (currently amended): A method for decrypting an encrypted computer program including at least one first block and a plurality of second blocks in sequence, the method comprising the steps of:

generating a first cipher key from the at least one first block of the encrypted computer program;

performing a first decryption ~~of a plurality~~ on each of the plurality of second blocks of the encrypted computer program with said first cipher key which is generated from the at least one first block; and

performing a second decryption ~~of~~ on each of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key.

Claim 7(previously presented): The method as set forth in claim 6,

wherein said at least one first block is not encrypted.

Claim 8 (previously presented): The method as set forth in claim 6,

wherein said plurality of second blocks are encrypted at least with said first cipher key prior to being decrypted.

Claim 9 (previously presented): The method as set forth in claim 8,

wherein at least one of said plurality of second blocks is encrypted with said second cipher key prior to being decrypted.

Claim 10 (previously presented): The method as set forth in claim 6, further comprising the steps of:

determining whether the encrypted computer program is analyzed; and

decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed.

Claim 11 (currently amended): A computer program product embodied on a computer-readable medium and comprising code that, when executed, causes a computer to perform a method for decrypting an encrypted computer program including at least one first block and a plurality of second blocks in sequence, said method comprising the steps of:

generating a first cipher key from the at least one first block of the encrypted computer program;

performing a first decryption ~~of a plurality~~ on each of the plurality of second blocks of the encrypted computer program with said first cipher key which is generated from the at least one first block; and

performing a second decryption ~~of~~ on each of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key.

Claim 12 (previously presented): The computer program product as set forth in claim 11, wherein said at least one first block is not encrypted.

Claim 13 (previously presented): The computer program product as set forth in claim 11, wherein said plurality of second blocks are encrypted at least with said first cipher key prior to being decrypted.

Claim 14 (previously presented): The computer program product as set forth in claim 13,

wherein at least one of said plurality of second blocks is encrypted with said second cipher key prior to being decrypted.

Claim 15 (previously presented): The computer program product as set forth in claim 11, wherein said method further comprises the steps of:

determining whether the encrypted computer program is analyzed; and

decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed.

Claims 16-19 (canceled).

Claim 20 (previously presented): The system as set forth in claim 1, wherein said means for performing the second decryption of the plurality of second blocks executes the second decryption faster than said means for performing the first decryption of the plurality of second blocks.

Claim 21 (previously presented): The method as set forth in claim 6, wherein said step of performing the second decryption of the plurality of second blocks is executed faster than said step of performing the first decryption of the plurality of second blocks.

Claim 22 (previously presented): The computer program as set forth in claim 11, wherein said step of performing the second decryption of the plurality of second blocks is executed faster than said step of performing the first decryption of the plurality of second blocks.